Cassandra Crossing/ Il Silenzio sul Grande Bug dell'Hardware

(445) La maggior parte degli iCosi già venduti sono vulnerabili senza possibilità di patch, ma la notizia non esce sui media generalisti…

Cassandra Crossing/ Il Silenzio sul Grande Bug dell'Hardware

(445) La maggior parte degli iCosi già venduti sono vulnerabili senza possibilità di patch, ma la notizia non esce sui media generalisti; perché?

5 dicembre 2019—Alcuni dei 24 inossidabili lettori di Cassandra avranno seguito, nelle chat di sviluppatori, di esperti di computer forensics o di hardware, una questione che sulla stampa estera specialistica ha dato luogo ad una manciata di articoli, ma che sui media tradizionali, particolarmente quelli italiani, è passata completamente sotto silenzio.

La notizia è tecnica, e si può riassumere dicendo che la bootrom della maggior parte dei prodotti Apple, inclusi gli iphone da 4 ad X, ha un bug che permette di prendere il controllo del telefono prima del boot di Ios.
In pratica puoi far fare al telefono quello che vuoi, incluso cose come leggere i file anche se il telefono è bloccato. Anche per dei prodotti che (meritatamente, credetemi) hanno la reputazione di essere molto più sicuri di altri.

La vulnerabilità si chiama Checkm8, e l'exploit, cioè il software che permette (ai buoni) di eseguire analisi forensi prima impossibili, e ad altri Cassandra non osa pensare cosa, si chiama Checkra1n (con "1" non con "l").

Niente link, googlate se vi interessano i dettagli.

Cassandra, che vede sempre le cose in prospettiva, non è interessata a questo bug, né tantomeno ai device che ne sono suscettibili, al loro numero, alla loro marca od alla reputazione della marca stessa (di cui in passato è stato anche sviluppatore).

No, l'interesse, anzi la preoccupazione, è che l'interpretazione che fa del silenzio su quest'evento sia esatta.

Pensateci. La bootrom, pur essendo un bug software, fa parte dell'hardware, poiché non è patchabile.

E' quindi un bug hardware, che ammette solo due soluzioni:

- [la prima, sostituire il prodotto;]
- [la seconda, far finta di nulla, sperando che nessuno si inc ^h^h^h si arrabbi troppo, rimediando all'eventuale pubblicità negativa ingaggiando una reputation agency.]

E potendo questo capitare in qualsiasi prodotto che contenga software, questo sarà probabilmente, nel prossimo futuro, il normale approccio di tutti i produttori di oggetti col cuore informatico come IoT, elettrodomestici, automobili, droni, smarthphone, televisori, LAWS (Armi Autonome Letali), qualsiasi cosa.

Ma gli utenti finali?
Quelli che hanno in mano un oggetto divenuto improvvisamente "pericoloso"?

Normalmente li chiamano "consumatori", cioè esseri eminentemente passivi e controllabili.
Ma se diventassero proprietari arrabbiati, come avrebbero tutto il diritto di fare, e membri di una class action?

E se questo succedesse per ogni prodotto a larga diffusione che si scoprisse irrimediabilmente fallato?

Cosa sperare per il futuro?

Che i consumatori reagiscano davvero? Ma dai…

Che il legislatore italiano incida efficacemente sul problema? Magari, ma il passato insegna …

Che l'Europa incida sulla realtà come nel caso degli alimentatori telefonini? Potrebbe essere, ma è come sperare che, dopo aver sconfitto un topolino, riesca a far polpette di un branco di T-Rex inferociti.

Ma una cosa fa paura anche ai T-Rex: le class action.

Adconsum, Altroconsumo, Codacons, siete in linea?

By Marco A. L. Calamari on May 19, 2022.

Canonical link

Exported from Medium on August 27, 2025.